CARLTON FIELDS

Decisions Highlight Split in Application of Computer Fraud and Abuse Act

April 24, 2013

Trade secret claims have historically derived from state common law causes of action and, subsequently, most states' adoption of the Uniform Trade Secrets Act, which codifies that common law and generally proscribes the misappropriation of trade secrets. In recent years, the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, has been used to invoke federal jurisdiction and to raise the specter of criminal, as well as civil, liability for "unauthorized access" to a "protected" computer, even where the trade secret misappropriation elements could not be met.

As the use of computers has become ubiquitous, litigants may attempt to pursue a private right of action under the CFAA for a multitude of innocuous situations, including an employee's use of an employer's computer for personal purposes. Recently, a rift has developed within the United States Court of Appeals with respect to the interpretation of the act, including whether it should be construed broadly or narrowly. Two circuit court decisions in 2012 highlight the trend to interpret the CFAA more restrictively.

In *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc), the Ninth Circuit, sitting en banc, overturned the court's initial decision on appeal and interpreted the CFAA narrowly. In that case, the United States brought criminal charges under the act against Daniel Nosal for convincing some of his former coworkers to help him start a competing business by downloading his former employer's confidential information and then providing it to him for use in his new business. Nosal was charged with aiding and abetting his former coworkers in "exceeding their authorized access" with intent to defraud. The trial court denied Nosal's motion to dismiss the CFAA charges brought against him. *United States v. Nosal*, No. CR 08-00237 MHP, 2009 WL 981336, at *7 (N.D. Cal. Apr. 13, 2009).

On appeal, the Ninth Circuit, sitting en banc, noted the challenges presented in the modern age of

computing:

> Computers have become an indispensable part of our daily lives. We use them for work; we use them for play. Sometimes we use them for play at work. Many employers have adopted policies prohibiting the use of work computers for nonbusiness purposes. Does an employee who violates such a policy commit a federal crime? How about someone who violates the terms of service of a social networking website? This depends on how broadly we read the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030.

Nosal, 676 F.3d at 856.

The court held that the phrase in the act referring to exceeding "authorized access" is limited to authority to access the computer, itself, and does not apply to "use" restrictions, such as a company policy requiring a computer to be used for furthering a company's business purposes only. *Id.* at 863. Thus, the court concluded that the United States' CFAA claims must be dismissed. *Id.*

The Ninth Circuit expressly disagreed with those decisions of other circuits, including the Fifth, Seventh, and Eleventh Circuits, that have interpreted the CFAA broadly. See *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); *United States v. John*, 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006). Noting that "[t]he rule of lenity requires penal laws … to be construed strictly," the Ninth Circuit found that "[w]hen choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite." *Nosal*, 676 F.3d at 863 (citations omitted).

Similarly, the Fourth Circuit Court of Appeals, in *WEC Carolina Energy Solutions, LLC v. Miller*, 2012 WL 3039213 (4th Cir. 2012), held that prohibited use does not constitute "unauthorized access" under the CFAA. In that case, a welding company brought a civil action against a former employee, the employee's assistant, and a competitor alleging that they violated the CFAA when the employee, before resigning and at the competitor's direction, downloaded the company's proprietary information and used it to prepare a presentation to a customer on behalf of the competitor. The WEC decision distinguished its ruling from the line of cases following *International Airport Centers, LLC v. Citrin*, 440 F.3d 418, 420–21 (7th Cir. 2006), which held that "when an employee accesses a computer or information on a computer to further interests that are adverse to his employer…[he] loses any authority he has to access the computer or any information on it."

The *WEC* court disagreed with this reasoning and ruled that because the defendant employees had authority to access the computers, their acts of downloading confidential documents may have violated the "use" policy but did not violate the CFAA. *Miller*, 687 F.3d at 206–7.

Given that an increasing number of trade secret misappropriation cases and breach of employment contract cases include CFAA claims, this conflict within the Court of Appeals warrants intervention and resolution by the Supreme Court, by Congress, or by both. *This article was originally published in Business Torts Litigation, ABA Section of Litigation, Spring 2013, Vol. 20, No. 3 (April 23, 2013).*

Related Practices

Intellectual Property
Trade Secrets / Noncompete Litigation and Consulting